2-adic properties of the number of solutions $x^m=1$ in the alternating group A_n (Research on finite groups and their representations, vertex operator algebras, and algebraic combinatorics)

AUTHOR(S):

竹ヶ原, 裕元

数理解析研究所講究録
第1926巻 2014年 1-12

2-adic properties of the number of solutions $x^m = 1$ in the alternating group A_n

竹ヶ原　裕元

室蘭工業大学

1　序

n を自然数とする. 型が $(1^{r_1}, 2^{r_2}, \ldots, n^{r_n})$ である n 次の置換の個数は

$$\frac{n!}{1^{r_1}r_1!2^{r_2}r_2!\cdots n^{r_n}r_n!}$$

である (cf. [10, Lemma 1.2.15], [16, Chap. 4 §2]). このことから

$$\sum \frac{n!}{1^{r_1}r_1!2^{r_2}r_2!\cdots n^{r_n}r_n!} = |S_n|(= n!)$$

が成り立つ. ここで和は n 次の置換の型 $(1^{r_1}, 2^{r_2}, \ldots, n^{r_n})$ 全体を動く. この式は

$$\begin{aligned} 1 + x + x^2 + \cdots &= (1-x)^{-1} = \exp(-\log(1-x)) \\ &= \exp\left(x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots\right), \qquad |x| < 1 \end{aligned}$$

からも導かれる. m を自然数とし, S_n における方程式 $x^m = 1$ の解の個数を $a_n(m)$ で表す. すなわち

$$a_n(m) = \sharp\{\sigma \in S_n \mid \sigma^m = 1\}$$

であり, $a_n(m)$ は位数が m の約数である n 次の置換の個数である. また $a_0(m) = 1$ とし, $\{\ell_0, \ell_1, \ldots, \ell_s\}$ を m の約数全体の集合とする. 位数が m の約数である n 次の置換の型を考えれば

$$\sum_{n=0}^{\infty} \frac{a_n(m)}{n!} X^n = \exp\left(\sum_{k=0}^{s} \frac{1}{\ell_k} X^{\ell_k}\right) \tag{I}$$

が成り立つ (cf. [2]). この式の両辺を微分すれば, 漸化式

$$a_n(m) = \sum_{k=0}^{s} \frac{(n-1)!}{(n-\ell_k)!} a_{n-\ell_k}(m)$$

も得られる. ただし $a_{-n}(m) = 0$, $n \in \mathbb{N}$, である. 特に, 素数 p について

$$a_n(p) = a_{n-1}(p) + (n-1)(n-2)\cdots(n-p+1)a_{n-p}(p)$$

である. p を素数とし, 0 でない整数 a に対して, a を割り切る最大の p のべき数を $\mathrm{ord}_p(a)$ で表す. 実数 x に対して $[x]$ で x を超えない最大の整数を表すとき, これらの式を用いて

$$\mathrm{ord}_p(a_n(p)) \geq \left[\frac{n}{p}\right] - \left[\frac{n}{p^2}\right]$$

が示される (cf. [3, 5, 6, 8, 9]). $p = 2$ の場合, この式は Chowla–Herstein–Moore [1] により示されたが, より正確には

$$\mathrm{ord}_2(a_n(2)) = \begin{cases} \left[\frac{n}{2}\right] - \left[\frac{n}{4}\right] + 1, & n \equiv 3 \pmod 4 \quad \text{の場合,} \\ \left[\frac{n}{2}\right] - \left[\frac{n}{4}\right] & \text{その他の場合,} \end{cases} \tag{II}$$

が証明される (cf. [5, 15]). また D. Kim–J. S. Kim [12] はこれらの結果を置換の数え上げにより直接示した.

A_n における方程式 $x^m = 1$ の解の個数を $t_n(m)$ で表す. すなわち

$$t_n(m) = \sharp\{\sigma \in A_n \mid \sigma^m = 1\}$$

であり, $t_n(m)$ は位数が m の約数である n 次偶置換の個数である. $\sigma^m = \epsilon$ を満たす n 次偶置換 σ の型 $(\ell_0^{j_0}, \ell_1^{j_1}, \ldots, \ell_s^{j_s})$ は, ℓ_i が偶数である場合の j_i の和が偶数であるものに限る. また

$$\exp\left(\sum_{k=0}^{s}(-1)^{\ell_k-1}\frac{1}{\ell_k}X^{\ell_k}\right) = \sum_{n=0}^{\infty}\sum_{j_0\ell_0+j_1\ell_1+\cdots+j_s\ell_s=n}\frac{(-1)^{\sum_{\ell_k\text{が偶数}} j_k}}{\ell_0^{j_0}j_0!\ell_1^{j_1}j_1!\cdots\ell_s^{j_s}j_s!}X^n$$

である. よって

$$\sum_{n=0}^{\infty}\frac{t_n(m)}{n!}X^n = \frac{1}{2}\left\{\exp\left(\sum_{k=0}^{s}\frac{1}{\ell_k}X^{\ell_k}\right) + \exp\left(\sum_{k=0}^{s}(-1)^{\ell_k-1}\frac{1}{\ell_k}X^{\ell_k}\right)\right\} \tag{III}$$

が得られる (cf. [16, Chap. 4, Problem 22]). 特に $m = 2$ ならば

$$\sum_{n=0}^{\infty}\frac{t_n(2)}{n!}X^n = \frac{1}{2}\left\{\exp\left(X + \frac{1}{2}X^2\right) + \exp\left(X - \frac{1}{2}X^2\right)\right\}$$

が成り立つ. この式を用いて $\mathrm{ord}_2(t_n(2))$ の性質が得られる. D. Kim–J. S. Kim [12] は置換の数え上げにより, 任意の非負整数 y に対して,

$$\mathrm{ord}_2(t_{4y}(2)) = y + \chi_o(y),\ \mathrm{ord}_2(t_{4y+2}(2)) = \mathrm{ord}_2(t_{4y+3}(2)) = y,$$

ここで $\chi_o(y) = 1$, y が奇数の場合, $\chi_o(y) = 0$, y が偶数の場合, が成り立つことを示し,

$$\mathrm{ord}_2(t_{4y+1}(2)) = y + \chi_o(y)\cdot(\mathrm{ord}_2(y+\alpha) + 1)$$

を満たす 2-進整数 α が存在することを予想した. この報告では予想が正しいことの証明およびその一般化について解説する.

2 母関数, アルティン・ハッセ指数関数

$\mathbb{Z}_p$ で p-進整数の環を表す. 次の結果はデュドネ [4] による.

命題 2.1 $\exp(\sum_{i=0}^{\infty} a_i X^{p^i}) = \sum_{n=0}^{\infty} c_n X^n$, $a_i \in \mathbb{Q}_p$ とする. このとき $c_n \in \mathbb{Z}_p$, $n = 1, 2, \ldots,$ であるための必要十分条件は

$$a_i - \frac{a_{i-1}}{p} \in \mathbb{Z}_p, \quad i = 0, 1, 2, \ldots, \qquad (a_{-1} = 0)$$

が成り立つことである.

以後, u を正の整数とする. 式 (I) より,

$$\sum_{n=0}^{\infty} \frac{a_n(p^u)}{n!} x^n = \exp\left(\sum_{k=0}^{u} \frac{1}{p^k} X^{p^k} \right) \tag{IV}$$

である. $a_n^0(p^u) = a_n(p^u)$ とおき, 数列 $\{a_n^1(p^u)\}_{n=0}^{\infty}$ を

$$\sum_{n=0}^{\infty} \frac{a_n^1(p^u)}{n!} X^n = \exp\left(-\sum_{k=0}^{u} \frac{1}{p^k} X^{p^k} \right) \tag{V}$$

により定める. $p = 2$ のとき, 式 (III) より,

$$t_n(2^u) = \frac{1}{2}(a_n^0(2^u) + (-1)^n a_n^1(2^u)) \tag{VI}$$

が成り立つ. $\natural$ は 0 または 1 とする. 数列 $\{c_{n,p}^{\natural}\}_{n=0}^{\infty}$ を

$$\sum_{n=0}^{\infty} c_{n,p}^{\natural} X^n = \exp\left((-1)^{\natural} \sum_{k=0}^{\infty} \frac{1}{p^k} X^{p^k} \right) \in 1 + X\mathbb{Z}_p[[X]]$$

により定める. 命題 2.1 より, $c_{n,p}^{\natural} \in \mathbb{Z}_p \cap \mathbb{Q}$ $(n = 1, 2, \ldots)$ である. $\natural = 0$ のとき, これはアルティン・ハッセ指数関数と呼ばれる (cf. [4], [13, Chap. IV §2], [17, §48]). 簡単のため $c_n^{\natural} = c_{n,p}^{\natural}$ とおく.

補題 2.2 $0 \leqq r \leqq 17$ である整数 r について, $c_{r,2}^{\natural}$ の値は次の通りである (計算は Mathematica による).

r	0	1	2	3	4	5	6	7	8	9	10	11
$c_{r,2}^0$	1	1	1	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{7}{15}$	$\frac{16}{45}$	$\frac{67}{315}$	$\frac{88}{315}$	$\frac{617}{2835}$	$\frac{2626}{14175}$	$\frac{18176}{155925}$
$c_{r,2}^1$	1	-1	0	$\frac{1}{3}$	$-\frac{1}{3}$	$\frac{1}{5}$	$\frac{1}{45}$	$-\frac{5}{63}$	$-\frac{8}{105}$	$\frac{43}{405}$	$-\frac{74}{14175}$	$-\frac{559}{17325}$

r	12	13	14	15	16	17
$c^0_{r,2}$	$\frac{6949}{66825}$	$\frac{423271}{6081075}$	$\frac{2172172}{42567525}$	$\frac{19151162}{638512875}$	$\frac{58438907}{638512875}$	$\frac{899510224}{10854718875}$
$c^1_{r,2}$	$\frac{697}{18711}$	$-\frac{13232}{552825}$	$-\frac{30727}{14189175}$	$\frac{450991}{49116375}$	$-\frac{5519014}{91216125}$	$\frac{8250311}{144729585}$

以後, r を $0 \leqq r < p^{u+1}$ を満たす整数とする. 式 (IV) および (V) より

$$\sum_{n=0}^{\infty} \frac{a^{\natural}_n(p^u)}{n!} X^n = \left(\sum_{n=0}^{\infty} c^{\natural}_n X^n \right) \exp\left(-(-1)^{\natural} \sum_{i=0}^{\infty} \frac{1}{p^{u+i+1}} X^{p^{u+i+1}} \right)$$

である. また, この式から $X^{p^{u+1}y+r}$, $y = 0, 1, 2, \ldots,$ の項を取り出して X^r を約せば,

$$\sum_{y=0}^{\infty} \frac{a^{\natural}_{p^{u+1}y+r}(p^u)}{(p^{u+1}y+r)!} X^{p^{u+1}y} = \left(\sum_{j=0}^{\infty} c^{\natural}_{p^{u+1}j+r} X^{p^{u+1}j} \right) \times \exp\left(-(-1)^{\natural} \sum_{i=0}^{\infty} \frac{1}{p^{u+i+1}} X^{p^{u+i+1}} \right)$$

となる. さらに $X^{p^{u+1}}$ を $(-(-1)^{\natural} p^{u+1})X$ に置き換えて

$$\sum_{y=0}^{\infty} \frac{a^{\natural}_{p^{u+1}y+r}(p^u)}{(p^{u+1}y+r)!} (-(-1)^{\natural} p^{u+1})^y X^y = \left(\sum_{j=0}^{\infty} c^{\natural}_{p^{u+1}j+r} (-(-1)^{\natural} p^{u+1})^j X^j \right) \times \exp\left(-(-1)^{\natural} \sum_{i=0}^{\infty} \frac{(-(-1)^{\natural} p^{u+1})^{p^i}}{p^{u+i+1}} X^{p^i} \right)$$

を得る. 以後,

$$H^{\natural}_r(p^u) = \sum_{y=0}^{\infty} \frac{a^{\natural}_{p^{u+1}y+r}(p^u)}{(p^{u+1}y+r)!} (-(-1)^{\natural} p^{u+1})^y X^y$$

とおく. 数列 $\{e^{\natural}_n\}_{n=0}^{\infty}$ および $\{d^{\natural}_{n,r}\}_{n=0}^{\infty}$ を

$$\sum_{n=0}^{\infty} e^{\natural}_n X^n = \exp\left(\sum_{i=2}^{\infty} \frac{(-(-1)^{\natural})^{\delta_{2p}} p^{p^i(u+1)}}{p^{u+i+1}} X^{p^i} \right),$$

$$\sum_{n=0}^{\infty} d^{\natural}_{n,r} X^n = \left(\sum_{j=0}^{\infty} c^{\natural}_{p^{u+1}j+r} (-(-1)^{\natural} p^{u+1})^j X^j \right) \times \exp\left(\frac{(-(-1)^{\natural})^{\delta_{2p}} p^{p(u+1)}}{p^{u+2}} X^p \right) \sum_{n=0}^{\infty} e^{\natural}_n X^n$$

により定めるとき, 次の補題が成り立つ. ここで δ はクロネッカーのデルタである.

補題 2.3 [14] $H^{\natural}_r(p^u) = \exp(X) \sum_{n=0}^{\infty} d^{\natural}_{n,r} X^n$

3 p-進解析からの準備

形式的べき級数環 $\mathbb{Z}_p[[X]]$ の部分環 $\mathbb{Z}_p\langle X\rangle$ を

$$\mathbb{Z}_p\langle X\rangle = \left\{ \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Z}_p[[X]] \;\middle|\; \lim_{n\to\infty} |a_n|_p = 0 \right\}$$

とする. $g(X) = \sum_{n=0}^{\ell} g_n X^n \in \mathbb{Z}_p[X]$ に対して, $f(X) = g(X) + p^{k_1} X^{k_2} h(X)$, $h(X) \in \mathbb{Z}_p\langle X\rangle$, k_1, k_2 は非負整数, と表される形式的べき級数の集合を $g(X) + p^{k_1} X^{k_2} \mathbb{Z}_p\langle X\rangle$ で表す. $c^{\natural}_{p^{u+1}j+r} \in \mathbb{Z}_p$, $j = 0, 1, 2, \ldots$, より,

$$\sum_{j=0}^{\infty} c^{\natural}_{p^{u+1}j+r} (-(-1)^{\natural} p^{u+1})^j X^j \in \mathbb{Z}_p\langle X\rangle$$

である. 次の 3 補題を用いる.

補題 3.1 ([7, Problems 164 and 165], [13, p. 7, Exercise 14], [17, Lemma 25.5]) $n = n_0 + n_1 p + n_2 p^2 + \cdots \in \mathbb{N}$, $n_i \in \{0, 1, \ldots, p-1\}$, とすると,

$$\mathrm{ord}_p(n!) = \sum_{j=1}^{\infty} \left[\frac{n}{p^j} \right] = \frac{n - n_0 - n_1 - n_2 - \cdots}{p-1} \leqq \frac{n-1}{p-1}$$

である.

補題 3.2 ([14]) k を正の整数とし, a を $\mathrm{ord}_p(a) = k$ である整数とする. $p \geqq 3$ または $k \geqq 2$ とする. このとき

$$\exp(aX) \in 1 + aX + \frac{a^2}{2} X^2 + \frac{a^3}{6} X^3 + p^{2k+1} X^4 \mathbb{Z}_p\langle X\rangle$$

が成り立つ.

補題 3.3 ([14]) $m_0 + m_1 X + \cdots + m_\ell X^\ell \in \mathbb{Z}_p[X]$, k を非負整数, $\sum_{n=1}^{\infty} w_n X^n \in p^k X \mathbb{Z}_p\langle X\rangle$, $\sum_{n=1}^{\infty} d_n X^n = m_0 + m_1 X + \cdots + m_\ell X^\ell + \sum_{n=1}^{\infty} w_n X^n$ とする. このとき

$$g(X) \in \sum_{i=0}^{\ell} m_i i! \binom{X}{i} + p^k X \mathbb{Z}_p\langle X\rangle, \qquad \sum_{n=0}^{\infty} \frac{g(n)}{n!} X^n = \exp(X) \sum_{n=0}^{\infty} d_n X^n$$

を満たす $g(X) \in \mathbb{Z}_p\langle X\rangle$ が存在する. ここで

$$\binom{X}{i} = \frac{X(X-1)\cdots(X-i+1)}{i!}, \quad i = 1, 2, \ldots, \quad \binom{X}{0} = 1$$

である.

4 対称群における $x^{p^u}=1$ の解の個数に関する p-進的性質

補題 3.2 より, 次の補題が得られる.

補題 4.1 ([14]) $\displaystyle\sum_{n=0}^{\infty} e_n X^n \in 1+p^{3u+1}X\mathbb{Z}_p\langle X\rangle$

補題 2.3, 3.2, 3.3, 4.1 より, 次の定理が得られる.

定理 4.2 ([14]) $p \geqq 3$ とする. このとき

$$g_r(y)=\frac{a_{p^{u+1}y+r}(p^u)}{(p^{u+1}y+r)!}(-p^{u+1})^y y!, \qquad y=0,\,1,\,2,\ldots,$$

$$g_r(X) \in c_r^0 - c_{p^{u+1}+r}^0 p^{u+1}X + p^{2u+1}X\mathbb{Z}_p\langle X\rangle$$

を満たす $g_r(X)\in\mathbb{Z}_p\langle X\rangle$ が存在する.

$p=2$ の場合の結果を述べる. 補題 2.3, 3.2, 3.3, 4.1 より, 次の定理が得られる.

定理 4.3 ([14]) $p=2$, $u \geqq 2$ とする. このとき

$$g_r^\natural(y)=\frac{a_{2^{u+1}y+r}^\natural(2^u)}{(2^{u+1}y+r)!}(-(-1)^\natural 2^{u+1})^y y!, \qquad y=0,\,1,\,2,\ldots,$$

$$\begin{aligned} g_r^\natural(X) \in c_r^\natural(1-(-1)^\natural 2^u X(X-1)+2^{2u-1}X(X-1)(X-2)(X-3)) \\ -(-1)^\natural c_{2^{u+1}+r}^\natural 2^{u+1}X + 2^{2u+1}X\mathbb{Z}_2\langle X\rangle \end{aligned}$$

を満たす $g_r^\natural(X)\in\mathbb{Z}_2\langle X\rangle$ が存在する.

補題 2.3, 3.1, 3.2, 4.1 と定理 4.3 より, 次の定理が得られる.

定理 4.4 ([14]) $p=2$, $u=1$ とする. このとき

$$g_r^\natural(y)=\frac{a_{4y+r}^\natural(2)}{(4y+r)!}((-1)^\natural 4)^y y!, \qquad y=0,\,1,\,2,\ldots,$$

$$\begin{aligned} g_r^\natural(X) \in c_r^\natural(1-2X+4\delta_{\natural 1}X(X-1)-4X(X-1)(X-2)(X-3)) \\ +(-1)^\natural 4c_{4+r}^\natural X + 8X\mathbb{Z}_2\langle X\rangle \end{aligned}$$

を満たす $g_r^\natural(X)\in\mathbb{Z}_2\langle X\rangle$ が存在する.

定義から $a_r(p^u)/r! = c_r^0$ である. また, 補題 3.1 より

$$\begin{aligned}\mathrm{ord}_p\left(\frac{(p^{u+1}y+r)!}{p^{(u+1)y}y!}\right) &= \sum_{j=1}^{u}\left[\frac{p^{u+1}y+r}{p^j}\right] - uy \\ &= \left\{\frac{p^{u+1}-1}{p-1} - (u+1)\right\}y + \mathrm{ord}_p(r!)\end{aligned}$$

が成り立つ. また, $n = p^{u+1}y + r$ とすれば, $y = [n/p^{u+1}]$ であり,

$$\mathrm{ord}_p\left(\frac{n!}{p^{(u+1)[n/p^{u+1}]}[n/p^{u+1}]!}\right) = \sum_{j=1}^{u}\left[\frac{n}{p^j}\right] - u\left[\frac{n}{p^{u+1}}\right]$$

となる. 定理 4.2, 4.3, 4.4 より, 次の系が成り立つ.

系 4.5 ([11, 14]) y を非負整数とする. このとき

$$\mathrm{ord}_p\left(a_{p^{u+1}y+r}(p^u)\right) \geqq \sum_{j=1}^{u}\left[\frac{p^{u+1}y+r}{p^j}\right] - uy$$

である. また $\mathrm{ord}_p(a_r(p^u)) \leqq \mathrm{ord}_p(r!) + u$ ($\Longleftrightarrow \mathrm{ord}_p(c_r^0) \leqq u$) ならば

$$\begin{aligned}\mathrm{ord}_p(a_{p^{u+1}y+r}(p^u)) &= \sum_{j=1}^{u}\left[\frac{p^{u+1}y+r}{p^j}\right] - uy + \mathrm{ord}_p(c_r) \\ &= \left\{\frac{p^{u+1}-1}{p-1} - (u+1)\right\}y + \mathrm{ord}_p(a_r(p^u))\end{aligned}$$

となる.

例 4.6 $a_0(2) = a_1(2) = 1$, $a_2(2) = 2$, $a_3(2) = 4$ より, (II) が得られる.

補題 2.2, 定理 4.3, 系 4.5 より, 次の命題が得られる.

命題 4.7 ([14]) $p = 2$, $u = 2$ とする. このとき, $y = 0, 1, 2, \ldots,$ に対して,

$$\begin{aligned}\mathrm{ord}_2(a_{8y+r}(4)) &= \left[\frac{8y+r}{2}\right] + \left[\frac{8y+r}{4}\right] - 2y + \mathrm{ord}_2(c_r) \\ &= 4y + \mathrm{ord}_2(r!) + \mathrm{ord}_2(c_r),\end{aligned}$$

すなわち

r	0	1	2	3	4	5	6	7
$\mathrm{ord}_2(a_{8y+r}(4)) - 4y$	0	0	1	2	4	3	8	4

が成り立つ.

5 交代群における $x^{2^u}=1$ の解の個数に関する 2-進的性質

次の定理は p-進ワイエルシュトラスの予備定理と呼ばれる (cf. [7, Theorem 6.2.6]).

定理 5.1 形式的べき級数 $f(X)=\sum f_nX^n\in\mathbb{Z}_p[[X]]$ は $\lim_{n\to\infty}|f_n|_p=0$ を満たすとする. N を $|f_N|_p=\max|f_n|_p$ かつすべての $n>N$ について $|f_n|_p<|f_N|_p$ を満たす整数とする. このとき N 次多項式

$$k_0+k_1X+k_2X^2+\cdots+k_NX^N\in\mathbb{Q}_p[X]$$

と形式的べき級数

$$1+m_1X+m_2X^2+\cdots\in\mathbb{Q}_p[[X]]$$

が存在して, 次が成り立つ.

(1) $f(X)=(k_0+k_1X+k_2X^2+\cdots+k_NX^N)(1+m_1X+m_2X^2+\cdots)$

(2) $|k_N|_p=\max|k_n|_p$

(3) $\lim_{n\to\infty}|m_n|_p=0$

(4) $|m_n|_p<1$, $^\forall n\geqq 1$

非負整数 y に対して $\chi_o(y)=(1+(-1)^{y+1})/2$ とおく.

定理 5.2 ([14]) $p=2$, $u=1$ とする. このとき, 任意の非負整数 y に対して次が成り立つ.

(a) $\mathrm{ord}_2(t_{4y}(2))=y+\chi_o(y)$, $\mathrm{ord}_2(t_{4y+2}(2))=\mathrm{ord}_2(t_{4y+3}(2))=y$.

(b) $\mathrm{ord}_2(t_{4y+1}(2))=y+\chi_o(y)\cdot(\mathrm{ord}_2(y+\alpha)+1)$ を満たす $\alpha\in\mathbb{Z}_2$ が存在する.

証明の概略. 定理 4.4 の記号を用いる. y を非負整数とする. (VI) より

$$t_{4y+r}(2)=\frac{(4y+r)!}{4^y\cdot y!}\cdot\frac{g_r^0(y)+(-1)^{r+y}g_r^1(y)}{2}$$

である. $L_{r,y}(X)=(g_r^0(X)+(-1)^{r+y}g_r^1(X))/2$ とおく. このとき, 補題 2.2 より, y が偶数のとき

$$L_{0,y}(y)\equiv L_{1,y}(y)\equiv 1 \pmod 4,$$
$$L_{2,y}(y)\equiv\frac{1}{2} \pmod 2,\quad L_{3,y}(y)\equiv\frac{1}{6} \pmod 4,$$

y が奇数のとき

$$L_{0,y}(y) \equiv -2y^2 \pmod 4, \quad L_{1,y}(y) \equiv \frac{38}{15}y - 2y^2 \pmod 4,$$
$$L_{2,y}(y) \equiv \frac{1}{2} - y \pmod 2, \quad L_{3,y}(y) \equiv \frac{1}{2} - y \pmod 4$$

となる. よって, $\mathrm{ord}_2((4y+r)!/4^y \cdot y!) = y + \mathrm{ord}_2(r!)$ より, (a) を得る. y が奇数とする. このとき

$$L_{1,y}(X) = -2X(X-1) + \frac{8}{15}X + 4XM_{1,y}(X) = \frac{38}{15}X - 2X^2 + 4XM_{1,y}(X)$$

を満たす $M_{1,y}(X) \in \mathbb{Z}_2\langle X \rangle$ が存在する. 定理 5.1 より 2 次多項式

$$k_0 + k_1X + k_2X^2 \in \mathbb{Q}_2[X]$$

と形式的べき級数

$$1 + m_1X + m_2X^2 + \cdots \in \mathbb{Q}_2[[X]]$$

が存在して (1)–(4) (ただし $f(X) = L_{1,y}(X)$, $N = 2$, $p = 2$) を満たす. $\lambda = 2^{-1}k_2$ とおく. $\mathrm{ord}_2(m_1) > 0$ だから, $\mathrm{ord}_2(\lambda) = 0$ である. さらに $\alpha := 2^{-1}k_1\lambda^{-1} \in \mathbb{Z}_2$ かつ

$$L_{1,y}(X) = 2\lambda X(X+\alpha)(1 + m_1X + m_2X^2 + \cdots)$$

が成り立つ. 結局

$$\mathrm{ord}_2(t_{4y+1}) = y + 1 + \mathrm{ord}_2(y+\alpha)$$

を得る. これより (b) が成り立つ. □

注意 5.3 定理 5.2(a) は [12] で示された. 定理 5.2(b) は [12] で予想され, [14] で示された. Mathematica による計算で $\alpha \equiv 1+2+2^3+2^8+2^{10}+2^{12} \pmod{2^{14}}$ がわかる.

$4y+1$	y	α	$\pmod{2^\sharp}$	$\mathrm{ord}_2(y+\alpha)$
5	1	$1+2$	$\pmod{2^3}$	2
21	5	$1+2+2^3$	$\pmod{2^5}$	4
85	21	$1+2+2^3$	$\pmod{2^6}$	5
213	53	$1+2+2^3$	$\pmod{2^7}$	6
469	117	$1+2+2^3$	$\pmod{2^8}$	7
981	245	$1+2+2^3+2^8$	$\pmod{2^{10}}$	9
3029	757	$1+2+2^3+2^8+2^{10}$	$\pmod{2^{12}}$	11
11221	2805	$1+2+2^3+2^8+2^{10}+2^{12}$	$\pmod{2^{14}}$	13

最後に $p=2, u \geqq 2$ の場合の結果を述べる.

定理 5.4 ([14]) $p=2, u \geqq 2$ とする. $r=0$ または $r=1$ ならば, 任意の非負整数 y に対して

$$\mathrm{ord}_2(t_{2^{u+1}y+r}(2^u)) = (2^{u+1}-u-2)y + \chi_o(y)\cdot(\mathrm{ord}_2(y+\alpha_r)+u)$$

となる $\alpha_r \in \mathbb{Z}_2$ が存在する. さらに, $\mathrm{ord}_2(c^0_{2^{u+1}+r} + (-1)^r c^1_{2^{u+1}+r}) = 0$, ならば

$$\mathrm{ord}_2(t_{2^{u+1}y+r}(2^u)) = (2^{u+1}-u-2)y + \chi_o(y)\cdot u$$

が成り立つ.

例 5.5 $p=2, u=2$ のとき, Mathematica による計算で次がわかる.

$$\alpha_0 \equiv 1+2+2^2+2^3+2^4+2^5+2^7+2^9+2^{10}+2^{12}+2^{13}+2^{14}+2^{15} \pmod{2^{17}}$$

$$\alpha_1 \equiv 1+2+2^4+2^7+2^8 \pmod{2^{12}}$$

$8y$	y	α_0	$(\mathrm{mod}\ 2^\sharp)$	$\mathrm{ord}_2(y+\alpha_0)$
8	1	$1+2+2^2+2^3+2^4+2^5$	$(\mathrm{mod}\ 2^7)$	6
520	65	$1+2+2^2+2^3+2^4+2^5+2^7$	$(\mathrm{mod}\ 2^9)$	8
2568	321	$1+2+2^2+2^3+2^4+2^5+2^7+2^9+2^{10}$	$(\mathrm{mod}\ 2^{12})$	11
18952	2369	$1+2+2^2+2^3+2^4+2^5+2^7$ $+2^9+2^{10}+2^{12}+2^{13}+2^{14}+2^{15}$	$(\mathrm{mod}\ 2^{17})$	16

$8y+1$	y	α_1	$(\mathrm{mod}\ 2^\sharp)$	$\mathrm{ord}_2(y+\alpha_1)$
9	1	$1+2$	$(\mathrm{mod}\ 2^3)$	2
41	5	$1+2$	$(\mathrm{mod}\ 2^4)$	3
105	13	$1+2+2^4$	$(\mathrm{mod}\ 2^6)$	5
361	45	$1+2+2^4$	$(\mathrm{mod}\ 2^7)$	6
873	109	$1+2+2^4+2^7+2^8$	$(\mathrm{mod}\ 2^{10})$	9
4969	621	$1+2+2^4+2^7+2^8$	$(\mathrm{mod}\ 2^{11})$	10
13161	1645	$1+2+2^4+2^7+2^8$	$(\mathrm{mod}\ 2^{12})$	11

また, y を非負整数とし, $\chi_e(y) = 1-\chi_o(y)$ とおけば, 次が成り立つ.

$$\mathrm{ord}_2(t_{8y+2}(4)) = \mathrm{ord}_2(t_{8y+3}(4)) = 4y,\ \mathrm{ord}_2(t_{8y+4}(4)) = 4y+2,$$
$$\mathrm{ord}_2(t_{8y+5}(4)) = 4y+3+\chi_e(y),\ \mathrm{ord}_2(t_{8y+6}(4)) = 4y+3,$$
$$\mathrm{ord}_2(t_{8y+7}(4)) = 4y+4+\chi_e(y).$$

参考文献

[1] S. Chowla, I. N. Herstein, and W. K. Moore, On recursions connected with symmetric groups I, Canad. J. Math. **3** (1951), 328–334.

[2] S. Chowla, I. N. Herstein, and W. R. Scott, The solutions of $x^d = 1$ in symmetric groups, Norske Vid. Selsk. Forh. (Trondheim) **25** (1952), 29–31.

[3] K. Conrad, p-adic properties of truncated Artin-Hasse coefficients, 1998, preprint.

[4] J. Dieudonné, On the Artin-Hasse exponential series, Proc. Amer. Math. Soc. **8** (1957), 210–214.

[5] A. Dress and T. Yoshida, On p-divisibility of the Frobenius numbers of symmetric groups, 1991, preprint.

[6] B. Dwork, A note on the p-adic gamma function, Groupe d'étude d'Analyse ultramétrique, 9e année, 1981/82, fasc. 3, n° J5, 10 pp.

[7] F. Q. Gouvêa, p-adic Numbers, 2nd ed., Universitext, Springer-Verlag, New York, 1997.

[8] M. Grady and M. Newman, Residue periodicity in subgroup counting functions; in :"The Rademacher Legacy to Mathematics," Contemp. Math. **166** (1994), 265–273.

[9] H. Ishihara, H. Ochiai, Y. Takegahara, and T. Yoshida, p-divisibility of the number of solutions of $x^p = 1$ in a symmetric group, Ann. Comb. **5** (2001), 197–210.

[10] G. D. James and A. Kerber, The Representation Theory of the Symmetric Group, Encyclopedia of mathematics and its applications, Vol. 16, Addison-Wesley, Reading, MA, 1981.

[11] H. Katsurada, Y. Takegahara, and T. Yoshida, The number of homomorphisms from a finite abelian group to a symmetric group, Comm. Algebra **28** (2000), 2271–2290.

[12] D. Kim and J. S. Kim, A combinatorial approach to the power of 2 in the number of involutions, J. Combin. Theory Ser. A **117** (2010), 1082–1094.

[13] N. Koblitz, p-adic Numbers, p-adic Analysis, and Zeta-Functions, 2nd ed., Springer-Verlag, New York, 1984.

[14] T. Koda, M. Sato, and Y. Takegahara, 2-adic properties for the numbers of involutions in the alternating groups, submitted.

[15] H. Ochiai, A p-adic property of the Taylor series of $\exp(x + x^p/p)$, Hokkaido Math. J. **28** (1999), 71–85.

[16] J. Riordan, An Introduction to Combinatorial Analysis, Wiley, New York, 1958.

[17] W. H. Schikhof, Ultrametric Calculus, Cambridge University Press, Cambridge, 1984.